Cyber Security Awareness Month Presentation
Your Privacy Is At Risk: Protecting Your Identity Online

Welcome (Slide 1)
Welcome to a short information security lesson, "Your Privacy Is At Risk: Protecting Your Identity Online." This tutorial is brought to you by the State of Tennessee's Security Management Group to promote Cyber Security Awareness Month.

Lesson Introduction (Slide 2)
This lesson will have five sections: shopping online, passwords for online accounts, selecting passwords, phishing scams and public wireless networks. At the end of the lesson there is a resource page incase you would like additional information.

Section One: Shopping Online (Slide 3)
When shopping online it is sometimes hard to know who exactly you are doing business with. Therefore, one good online practice is to verify that the site's URL says "HTTPS," which is more secure than a "HTTP" site. You might be asking yourself, "What is really the difference between HTTP and HTTPS?" Without going into too much technological detail, the big difference is that HTTPS works in conjunction with SSL (Secure Socket Layer) which encrypts the data thus making the transfer of the data you submit online to the vendor more secure.

Another online practice is designating one credit card for your online transactions. Some benefits of designating one credit card for online transactions is that you can better monitor your account, and if your credit card number is stolen it is easier to cancel the card and have it replaced. Also, if you have to cancel the credit card your monthly and/or annual charges will not be disrupted; such as a gym membership or annual magazine renewals. In the event that you use a debit card and your information is stolen the banking account connected to that debit card can be affected. The account can be drained quickly, and resolution can take longer.

Section Two: Passwords for Online Accounts (Slide 4)
Passwords are like keys because they grant access to your online accounts just like a key gives you access to your locked house. In cases where you have more than one online account it is safer to use different passwords. "Why?" you might ask. If someone happens to obtain your password you might not know it right away. Which means the person with your password could gain access to all your accounts. If someone has access to your accounts it is easier for them to impersonate you.

A good option to help you remember your passwords is to use variations of the same password. For example, you could use "Tr#vel7" or "7Trav#l."

Section Three: Selecting Passwords (Slide 5)
A good password is only as good as your ability to remember the password without having to write it down and post it to your computer monitor. If you have many accounts and passwords to remember, password safe software is a good solution for storing your passwords in a safe location. Your passwords should be at least 8 characters long, and it should include numbers and special characters. It is never a good idea to use the names of your family members, pets or favorite sports teams because those things are easily guessed by those who know you. Finally, dictionary words in any language are bad passwords because tools called "password crackers" can be used against your account to guess your password. These password crackers try all the words in the dictionary, and they do not stop at English only words.

Section Four: Phishing Scams (Slide 6)
One of the most popular cyber scams is "phishing." Phishing scams are deceptive and criminal attempts to steal your login credentials, account numbers or other sensitive data. Phishing scams are the result of e-mails sent out to a wide range of e-mail addresses. The e-mails appear to be from reputable institutions like your bank, and there is a place to click on a link within the e-mail that will route you to a website that looks legitimate. That is why you should exercise good judgment, and never access your accounts through an e-mail link. Instead, you should manually type in the institution's website and access your account information as necessary.

Due to the fact that phishing has become a successful means of attaining account information by criminals, most financial institutions have stopped sending e-mails to their customers asking them to update account information. Therefore, you should delete the phishing scam e-mail, and do not respond back to the sender.

Section Five: Public Wireless Networks (Slide 7)
Public wireless networks (Wi-Fi or Wireless Hotspots) are convenient ways to catch up on the last news events, sports or general information gathering. However, you should exercise caution, and avoid if possible, when considering the use of public wireless networks to conduct financial transactions or instances where you are accessing your private information. The reason for this is that most public wireless networks are unencrypted and unsecure.

When accessing a public wireless network you should keep your computer's firewall on. Also, to protect the data on your computer you should disable file sharing before connecting to a public wireless network.

Conclusion (Slide 8)
Thank you for taking the time to learn how to protect your identity while you are online. Three recourses are available for additional information: The State of Tennessee's Enterprise Information Security Policies, US-CERT White Paper, and an article issued by CNN regarding safe online practices.